



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/872,077	06/01/2001	Lisa Amini	STL920000116US1	3841

24852 7590 06/29/2005

INTERNATIONAL BUSINESS MACHINES CORP  
IP LAW  
555 BAILEY AVENUE , J46/G4  
SAN JOSE, CA 95141

EXAMINER
----------

NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 06/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/872,077

Applicant(s)

AMINI ET AL.

Examiner

Andrew L. Nalven

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 05 April 2005.  
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-44 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-44 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
10) ☒ The drawing(s) filed on 15 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_.  
5) ☐ Notice of Informal Patent Application (PTO-152)  
6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. Claims 1-44 are pending.

### ***Response to Arguments***

2. Applicant's arguments filed 13 January 2005 have been fully considered but they are not persuasive.

3. Applicant has argued on pages 12-13 that the Mitty reference (US Patent No. 6,145,079) fails to anticipate claims 1-4, 7-10, and 15-18 because the Mitty reference is directed towards a non-streamed (non-chunked) environment whereas the present invention is directed towards either a streamed or non-streamed environment. Applicant further argues that the focus of Mitty is an electronic messaging system which differs from the focus of the present invention. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the intended use of the invention and the type of environment the inventions operate in) are not positively recited in the limitations of the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

4. Applicant has argued on page 14 that it would not have been obvious to use an untrusted system because the techniques were not known at the time the invention was

Art Unit: 2134

conceived. Examiner respectfully disagrees. Untrusted systems are well known in the art and have been prior to the date of the present invention was conceived. Further, no system can be fully trusted because all systems have some element of vulnerability to attack or to being compromised. Mitty's invention teaches a second computer performing encryption in the same manner that the present invention teaches in that a data element is encrypted first by a first computer system and then by a second computer system (Mitty, column 8 lines 48-51, M2 encrypted to form M3, column 12 lines 14-23, M9 encrypted to form M10). The second computer system does not view plaintext data and thus an untrusted second computer system would be compatible with the system of Mitty.

Applicant has argued on page 15 that the combination of Mitty and Bailey III US Patent No. 5,659,614 fails to render claims 6, 11, and 19 unpatentable because Bailey does not teach an environment using chunked data and because the subject matter of Bailey is non-analogous with that of the present invention. Examiner notes that as currently provided there are no positively recited limitations regarding chunked or unchunked data. Thus, Applicant's argument with respect to that allegation is not persuasive. In response to applicant's argument that Bailey is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Bailey discloses methods of encrypting and securing data and such methods are

Art Unit: 2134

reasonably pertinent to the present invention because the present invention is directed towards the encrypting and decrypting of data.

5. Applicant has argued on pages 15-16 that the Koopman Jr reference (RE36,181) fails to render claims 12-13 and 20-21 obvious because Koopman's disclosure focuses on automobile door lock technology and not the technology of the present invention. Examiner respectfully disagrees. The portions of Koopman cited by the Examiner are focused upon error correction of transmitted encrypted data and thus are relevant to the present invention. Applicant's further argues that Koopman's error correction is directed towards single-error error correction and thus it would not have been obvious to extend this teaching to error correction of chunked and non-chunked data. Examiner notes that as currently provided, there are no limitations requiring error correction of multiple bits. Thus, Examiner maintains that Koopman remedies the defects of Mitty with regards to the lack of teaching of repairing a data element without retransmission of said data.

### ***Claim Rejections - 35 USC § 102***

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

Art Unit: 2134

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-4, 7-10, 15-18, 23-26, 29-32, and 37-40 are rejected under 35

U.S.C. 102(e) as being anticipated by Mitty et al, US Patent No. 6,145,079. Mitty teaches a secure electronic transaction system using a trusted intermediary to perform electronic services.

8. With regards to claims 1, 7, 15, 23, 29, and 37, Mitty teaches a data element being statically encrypted with a static key (Mitty, column 8 lines 48-51, M2 encrypted to form M3), a data element being dynamically encrypted with a dynamic key (Mitty, column 12 lines 14-23, M9 encrypted to form M10), and a data element being decrypted with a dynamic key and a static key (Mitty, column 12 line 61 – column 13 line 17, decrypts M10 and M3).

9. With regards to claims 2, 8, 16, 24, 30, 38, Mitty teaches encryption with said static key being strong encryption (Mitty, column 8 lines 48-51).

10. With regards to claims 3, 9, 17, 25, 31, 39, Mitty teaches encryption with said dynamic key being weak encryption (Mitty, column 12 lines 14-23).

11. With regards to claims 4, 10, 18, 26, 32, 40, Mitty teaches a data element being encrypted with a static key on a first computer system (Mitty, column 8 lines 48-51, M2 encrypted to form M3, column 10 lines 9-16 intermediary receives package from sender), the data element being encrypted with the dynamic key on a second computer system (Mitty, column 12 lines 14-23, M9 encrypted to form M10 by intermediary computer system), and the data element being decrypted with the static key and dynamic key on a third computer system thereby encryption and decryption are

Art Unit: 2134

distributed between the first, second, and third computer systems (Mitty, column 12 line 61 – column 13 line 17, recipient/3<sup>rd</sup> computer system decrypts M10 and M3).

***Claim Rejections - 35 USC § 103***

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. Claims 5 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mitty et al US Patent No. 6,145,079.

14. With regards to claims 5 and 27, Mitty fails to teach the second computer being untrusted. Examiner contends that untrusted computers are well known in the art and it would have been obvious to a person of ordinary skill in the art to allow Mitty's system to work with untrusted computers because it offers the advantage of allowing interoperability with a far wider range of networks and systems.

15. Claims 6, 11, 19, 28, 33, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mitty et al US Patent No. 6,145,079 in view of Bailey III US Patent No. 5,659,614.

16. With regards to claims 6, 11, 19, 28, 33, and 41, Mitty teaches a data element being encrypted with a static key and a dynamic key on a first computer system (Mitty,

Art Unit: 2134

column 8 lines 48-51, M2 encrypted to form M3, column 9 lines 25-47 encrypted M5 to form M6), but fails to teach the data element being decrypted by the same dynamic key on a second computer system. Bailey teaches the data element being decrypted with the static key and the dynamic key on a second computer system (Bailey, column 6 lines 9-21, column 18 lines 53-55). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Bailey's method with Mitty's secure transaction system because it offers the advantage of helping ensure an attacker cannot decrypt data by acquiring a single key during a transmission from a source to destination (Bailey, column 6 lines 8-21).

17. Claims 12-13, 20-21, 34-35, and 42-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mitty et al US Patent No. 6,145,079 in view of Koopman Jr. et al Re 36,181. Koopman teaches a pseudorandom number generation system with cryptographic authentication.

18. With regards to claims 12-13, 20-21, 34-35 and 42-43, Mitty teaches the determination of whether a transmission failed (Mitty, column 6 lines 30-56, confirmation messages), but fails to teach the repairing of the data element without retransmission. Koopman teaches the repairing of the data element without retransmission (Koopman, column 16 lines 44-56). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Koopman's correction method with Mitty's secure transaction system because it offers the advantage of ensuring that



Art Unit: 2134

received data is correct and helping prevent attacks through repetitive application of numbers towards a receiver (Koopman, column 16 lines 44-56).

19. Claims 14, 22, 36, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mitty et al US Patent No. 6,145,079 and Bailey III US Patent No. 5,659,614 as applied to claims 11 and 19 above, and further in view of Koopman Jr. et al Re 36,181.

20. With regards to claims 14, 22, 36, and 44, Mitty as modified teaches the determination of whether a transmission failed (Mitty, column 6 lines 30-56, confirmation messages), but fails to teach the repairing of the data element without retransmission. Koopman teaches the repairing of the data element without retransmission (Koopman, column 16 lines 44-56). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Koopman's correction method with Mitty's modified secure transaction system because it offers the advantage of ensuring that received data is correct and helping prevent attacks through repetitive application of numbers towards a receiver (Koopman, column 16 lines 44-56).

### ***Conclusion***

21. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2134

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven



David Y. Jung  
Primary Examiner

  
6/24/05